UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

ALLIANCE FOR AUTOMOTIVE INNOVATION, Plaintiff, v. MAURA HEALEY, ATTORNEY GENERAL OF THE COMMONWEWALTH OF MASSACHUSETTS, in her official capacity, Defendant.	CIVIL ACTION NO. 1:20-cv-12090-DPW

DEFENDANT ATTORNEY GENERAL MAURA HEALEY'S TRIAL MEMORANDUM

MAURA HEALEY
ATTORNEY GENERAL

Robert E. Toone, BBO No. 663249
Eric A. Haskell, BBO No. 665533
Phoebe Fischer-Groban, BBO No. 687068
Julia Kobick, BBO No. 680194
Assistant Attorneys General
Christine Fimognari, BBO No. 703410
Special Assistant Attorney General
One Ashburton Place
Boston, Massachusetts 02108

Dated: June 4, 2021

CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provisions

Statutes

Rules and Regulations

Defendant Attorney General Maura Healey submits this Trial Memorandum pursuant to the Court's Order Regulating Non-Jury Civil Trial, in advance of the June 14, 2021 trial of this case. Because the preemption claims of the plaintiff Alliance for Automotive Innovation ("the Alliance") are without merit, its request for injunctive and declaratory relief should be denied, and judgment should enter in the Attorney General's favor.

I. THE ALLIANCE LACKS ASSOCIATIONAL STANDING.

The Alliance does not have standing to press its preemption claims because it has not established that "both the asserted claim[s] and the requested relief can be adjudicated without the participation of individual members as named plaintiffs." *Me. People's Alliance & Nat. Res. Def. Council v. Mallinckrodt, Inc.* 471 F.3d 277, 283 (1st Cir. 2006). In cases seeking equitable relief, associational standing "is inappropriate if adjudicating the merits of an association's claim requires the court to engage in a 'fact-intensive-individual inquiry.'" *N.H. Motor Transp. Ass'n v. Rowe*, 448 F.3d 66, 72 (1st Cir. 2006) (citation omitted). That is particularly so "where member circumstances differ and proof of them is important." *Pharm. Care Mgmt. Ass'n v. Rowe*, 429 F.3d 294, 314 (1st Cir. 2005). Def.'s Proposed Concls. of Law ("CL") ¶¶ 1-3.

The Alliance's preemption claims cannot be adjudicated without the participation of individual car manufacturers (OEMs) as named plaintiffs because, industry-wide, OEMs' technical capabilities and circumstances vary significantly, as does the ease with which different OEMs can comply with the 2020 Right to Repair Law. Although the Alliance initially proposed that four OEMs would participate in discovery as representative of the industry, it terminated two of those OEMs' participation when it became clear that those two OEMs would be subject to discovery. *See* ECF No. 139 at 19-20. There is no evidence that the remaining two OEMs—

General Motors (GM) and Fiat Chrysler Automobiles (FCA)—have an approach to cybersecurity and data access that is representative of OEMs in general. Indeed, the elaborate confidentiality procedures that the Alliance has insisted upon in this case are premised on the notion that a given OEM's cybersecurity controls are so unique that they ought not to be exposed to public view or view by other OEMs. And even with respect to GM and FCA alone, application of the 2020 Right to Repair Law involves materially "different factual scenarios," demonstrating that associational standing in this case is not proper. *Nat'l Ass'n of Gov't Employees v. Mulligan*, 914 F. Supp. 2d 10, 14 (D. Mass. 2012). CL ¶¶ 4-9.

II. THE ALLIANCE LACKS A RIGHT OF ACTION TO ASSERT A PREEMPTION CHALLENGE TO THE 2020 RIGHT TO REPAIR LAW.

The Alliance's claims also fail at the outset because the Alliance has identified no right of action that entitles it to pursue claims of conflict preemption under the Motor Vehicle Safety Act ("MVSA"), 49 U.S.C. § 30101, *et seq.*, or the Clean Air Act ("CAA"), 42 U.S.C. § 7401 *et seq*. A plaintiff's lack of cause of action may be raised at trial. Fed. R. Civ. P. 12(h)(2)(C).

The Supremacy Clause "does not create a cause of action," *Armstrong v. Exceptional Child Ctr., Inc.*, 575 U.S. 320, 325 (2015), nor is any claim based on the Supremacy Clause "cognizable under 42 U.S.C. § 1983," *Boston & Me. Corp. v. Town of Ayer*, 330 F.3d 12, 18 (1st Cir. 2003). To invoke the equitable powers of an Article III court, a plaintiff seeking to establish that federal law immunizes it from state regulation must identify a substantive "federal right that [it] possesses against" the defendant. *Va. Office for Prot. & Advocacy v. Stewart*, 563 U.S. 247, 260 (2011). Here, the Alliance has failed to identify any substantive federal right conferred on an OEM by the MVSA or CAA that is enforceable against states or state officials sued in their official capacity. CL ¶¶ 10-16.

To the contrary, both the MVSA and the CAA evince Congress's "intent to foreclose" the equitable relief requested by the Alliance in this case. *Armstrong*, 575 U.S. at 328 (internal quotation marks omitted). The two would-be preemptive sections of the MVSA cited by the Alliance—the recall notice provisions and the "make inoperative" provision—are enforceable by the Secretary of Transportation, not by private individuals through an individual right of action. 49 U.S.C. §§ 30118-30120, 30122(b)-(c). Indeed, the MVSA grants the United States Attorney General an exclusive right of action to enforce both sections of the MVSA. *Id.* § 30121(b), 30163(a). The would-be preemptive provision of the CAA cited by the Alliance—the similar "render inoperative" provision, 42 U.S.C. § 7522(a)(3)(A)—likewise provides an exclusive right of action to the United States to enforce the provision through civil litigation. *See* 42 U.S.C. § 7523(a)-(b). As the Supreme Court has explained, "the 'express provision of one method of enforcing a substantive rule suggests that Congress intended to preclude others.'" *Armstrong*, 575 U.S. at 328 (quoting *Alexander v. Sandoval*, 532 U.S. 275, 290 (2001)); *see also Thorne v. Pep Boys Manny Moe & Jack Inc.*, 980 F.3d 879, 892 (3d Cir. 2020) (the MVSA "favor[s] public over private enforcement"). Accordingly, the Alliance lacks a cause of action in equity to raise preemption claims for injunctive and declaratory relief under the Supremacy Clause, the MVSA, and the CAA. CL ¶¶ 17-27.

III. THE 2020 RIGHT TO REPAIR LAW IS NOT PREEMPTED AS A MATTER OF LAW.

On the merits, the Alliance's preemption claims under the MVSA and CAA fail as a matter of law, and judgment should enter for the Attorney General on that basis alone.

A. The Alliance Must Prove That There Are No Circumstances Under Which the 2020 Right to Repair Law Will Not Conflict with Federal Law.

This is a facial, pre-enforcement challenge to the 2020 Right to Repair Law, a statute that

was approved by 75% of Massachusetts voters in the November 2020 election. Def.'s Proposed Findings of Fact ("FF") ¶ 48; CL ¶ 28. As plaintiff, the Alliance has the burden to prove preemption. *Capron v. Office of Att'y Gen'l*, 944 F.3d 9, 13, 21 (1st Cir. 2019) (citation omitted), *cert. denied*, 141 S. Ct. 150 (2020). CL ¶ 54. Courts presume in implied preemption cases like this one that "the historic police powers of the States" are not superseded "unless that was the clear and manifest purpose of Congress." *Arizona v. United States*, 567 U.S. 387, 400 (2012) (citation omitted). This presumption reflects the fact that "the States are independent sovereigns in our federal system," as well as "the historic primacy of state regulation of matters of health and safety." *Medtronic, Inc. v. Lohr*, 518 U.S. 470, 485 (1996) (citation omitted); *see also In re Pharm. Indus. Average Wholesale Price Litig.*, 582 F.3d 156, 178 (1st Cir. 2009) (presumption against preemption "applies in any field in which there is a history of state law regulation, even if there is also a history of federal regulation") (citing *Wyeth v. Levine*, 555 U.S. 555, 565 n.3 (2009)). CL ¶¶ 58-62.

To prevail on its claims, the Alliance must show that there is "no possible set of conditions" under which the 2020 Right to Repair Law "would not conflict with federal law." *Cal. Coastal Comm'n v. Granite Rock Co.*, 480 U.S. 572, 580 (1987); *accord Pharm. Research & Mfrs. of Am. v. Concannon*, 249 F.3d 66, 77 (1st Cir. 2001), *aff'd*, 538 U.S. 644 (2003). Accordingly, in assessing the Alliance's preemption claims, this Court need not determine precisely how the 2020 Right to Repair Law will apply in Massachusetts, though it may properly give weight to the Attorney General's interpretation of the statute. *See, e.g.*, *Nat'l Org. for Marriage v. McKee*, 649 F.3d 34, 66 (1st Cir. 2011) ("'In evaluating a facial challenge to a state law, a federal court must . . . consider any limiting construction that a state court or enforcement agency has proffered.'") (citation omitted); *McGuire v. Reilly*, 386 F.3d 45, 55, 64 (1st Cir.

2004) (noting the "great weight" the District Court properly accorded the Attorney General's interpretation of buffer zone statute); Pl.'s Opp'n to Mot. to Dismiss, ECF No. 83 at 11 (acknowledging that the Attorney General can "provide a limiting construction of the [2020 Right to Repair Law] that would eliminate the statutory conflict alleged"); *see also* Section IV.B, *infra* (setting forth Attorney General's interpretation of the 2020 Right to Repair Law). And even where there remains "uncertainty about what the [challenged] law means . . . without the benefit of a definitive interpretation from the state courts, it would be inappropriate to assume [the law] will be construed in a way that creates a conflict with federal law." *Arizona*, 567 U.S. at 415. Rather, the state law must be "read to avoid [preemption] concerns" if possible. *Id.* at 413-14. CL ¶¶ 29-34.

The Alliance contends that compliance with the 2020 Right to Repair Law would be difficult and time-consuming for GM and FCA, possibly requiring substantial changes to the designs of their vehicles. As discussed below, that is false as a factual matter. But it is also immaterial as a legal matter. To establish a valid preemption claim based on impossibility, a plaintiff must show that compliance with both federal and state law is "a physical impossibility," *Arizona*, 567 U.S. at 399 (quoting *Fla. Lime & Avocado Growers, Inc. v. Paul*, 373 U.S. 132, 142-43 (1963))—not that the state law is difficult or costly to comply with on its own. *See also PLIVA, Inc. v. Mensing*, 564 U.S. 604, 620 (2011) ("The question for 'impossibility' [preemption] is whether the private party could independently do under federal law what state law requires of it."); *In re Methyl Tertiary Butyl Ether (MTBE) Prods. Liab. Litig.*, 725 F.3d 65, 99 (2d Cir. 2013) ("If there was *any* available alternative for complying with both federal and state law—even if that alternative was not the most practical and cost-effective—there is no impossibility preemption."). CL ¶¶ 63, 85.

B. The 2020 Right to Repair Law Does Not Conflict with the MVSA, Federal Motor Vehicle Safety Standards, or Non-Binding NHTSA Guidance.

1. NHTSA's non-binding guidance cannot preempt state law.

The authority on which the Alliance primarily relies in its complaint as the basis for its MVSA preemption claim—the cybersecurity guidance document issued by NHTSA—cannot preempt state law. In any preemption case, "the federal restrictions or rights that are said to conflict with state law must stem from either the Constitution itself or a valid statute enacted by Congress." *Kansas v. Garcia*, 140 S. Ct. 791, 801 (2020). Policy preferences and "brooding federal interest[s]" are insufficient to preempt state law. *Va. Uranium, Inc. v. Warren*, 139 S. Ct. 1894, 1901 (2019) (lead opinion of Gorsuch, J.). Rather, "only federal laws 'made in pursuance' of the Constitution, through its prescribed processes of bicameralism and presentment, are entitled to preemptive effect," and any evidence of preemptive purpose must be "sought in the text and structure of the statute at issue." *Id.* at 1907; *see also Good v. Altria Group*, 501 F.3d 29, 51 (1st Cir. 2007), *aff'd*, 555 U.S. 70 (2008) (rejecting conflict preemption claim based on agency policy that was not exercise of formal rulemaking authority). CL ¶¶ 64-67.

Here, the NHTSA guidance on which the Alliance relies is not a law or regulation but rather non-binding agency guidance with no legal effect. The guidance provides only a discussion of "voluntary best practices" and "non-binding guidance to the automotive industry." CL ¶¶ 76-77. It is NHTSA's policy that such guidance documents are "not intended to have the force or effect of law in [their] own right." CL ¶ 77. In fact, GM has advocated that NHTSA maintain its flexible, non-binding approach to cybersecurity. FF ¶ 131.

2. The 2020 Right to Repair Law is not preempted by the "make inoperative" provision of the MVSA or any FMVSS.

None of the federal motor vehicle safety standards ("FMVSS") cited by the Alliance

impliedly preempt the 2020 Right to Repair Law. An FMVSS impliedly preempts state law only if that law stands as an "'obstacle' to the accomplishment" of a "significant" objective of the federal regulation, *Williamson v. Mazda Motor of Am., Inc.*, 562 U.S. 323, 330 (2011) (quoting *Geier v. Am. Honda Motor Co.*, 529 U.S. 886 (2000)), or if it is "impossible for a private party to comply with both state and federal requirements," *English v. General Elec. Co.*, 496 U.S. 72, 79 (1990). CL ¶¶ 68-69.

The Alliance's obstacle preemption claim fails at the outset because it has no basis to claim that the FMVSS embody or adopt a significant federal objective on cybersecurity that is incompatible with the 2020 Right to Repair Law. To be valid, an FMVSS must "be practicable, meet the need for motor vehicle safety, and be stated in objective terms," 49 U.S.C. § 30111(a), and the "objective terms" requirement means that compliance with the standard must be measurable by instruments, demonstrable, and replicable. *Chrysler Corp. v. Dep't of Transp.*, 472 F.2d 659, 676 (6th Cir. 1972). Here, none of the FMVSS cited by the Alliance address the secure data access issues addressed in the 2020 Right to Repair Law, much less provide objective terms by which compliance could be measured. CL ¶¶ 70, 72-74.

Cybersecurity protections are also not mentioned in any of the FMVSS' stated objectives. As NHTSA itself has acknowledged, vehicle cybersecurity "is not covered by an existing Federal Motor Vehicle Safety Standard." CL ¶ 74. *See Sprietsma v. Mercury Marine*, 537 U.S. 51, 65 (2002) (agency's "decision not to regulate" particular safety issue "is fully consistent with an intent to preserve state regulatory authority pending the adoption of specific federal standards"); *Freightliner Corp. v. Myrick*, 514 U.S. 280, 289 (1995) ("it is not impossible for" a party "to comply with both federal and state law" when "there is simply no federal standard" for that party to comply with); *Durham v. County of Maui*, 696 F. Supp. 2d 1150, 1159 (D. Haw. 2010)

(plaintiff's side-impact airbag claims not preempted by vehicle safety standard that contained "no side-impact airbag requirements, much less conflicting ones"). CL ¶ 75. Both GM's Director of Product Cybersecurity and FCA's Global Head of Technical Compliance acknowledge that there is no FMVSS that governs cybersecurity. FF ¶¶ 134, 170.

Nor does the 2020 Right to Repair Law conflict with the "make inoperative" provision of the MVSA, 49 U.S.C. § 30122(b), such that it is impossible for an OEM such as GM or FCA to comply with both the state law and the MVSA. Section 30122(b) provides that OEMs and others "may not knowingly make inoperative any part of a device or element of design installed on or in a motor vehicle or motor vehicle equipment in compliance with an applicable motor vehicle safety standard." As a threshold matter, the Alliance's reliance on this provision defies logic, since OEMs must certify their vehicles as compliant with the FMVSS before they can sell them. 49 U.S.C. § 30115(a). In any event, the 2020 Right to Repair Law does not require removing or disabling safety equipment or features installed to comply with a motor vehicle safety standard. It does not direct any party, for example, to disable a vehicle's air bags, brake system, or accelerator control system. Further, as discussed, no motor vehicle safety standard covers vehicle cybersecurity or data access controls, and, accordingly, cybersecurity features are not "part of a device or element of design installed . . . in compliance with an applicable motor vehicle safety standard." Section 30122(b) does not preempt state laws that impact features that GM or FCA chooses to layer on top of safety equipment required by vehicle safety standards, but to which the standards do not apply. CL ¶¶ 86-89.

3. The 2020 Right to Repair Law is not preempted by the speculative possibility that NHTSA might order a recall in the future.

Nor can the 2020 Right to Repair Law be preempted on the speculative assumption that it

will invariably be implemented in violation of hypothetical future NHTSA recall orders. It is improper in the preemption context to speculate that a state law "will be construed in a way that creates a conflict with federal law" or a federal agency's future enforcement actions. *Arizona*, 567 U.S. at 415. Quite the contrary: our system of cooperative federalism presumes that federal and state officials will apply overlapping laws in a way that avoids unnecessary conflict. *See Wright's Case*, 486 Mass. 98, 108, 156 N.E.3d 161, 171-72 (2020) (Massachusetts courts must "avoid conflict with Federal law and possible preemption under the supremacy clause"). The Alliance's contention that NHTSA's authority to address safety risks through recalls preempts any state law that touches on vehicle safety issues is also contradicted by the MVSA's saving clause, which provides that the recall remedy under §§ 30118-30121 of the Act "is in addition to other rights and remedies under other laws of the United States or a State." 49 U.S.C. § 30103(d). *See Chamberlan v. Ford Motor Co.*, 314 F. Supp. 2d 953, 960, 964 (N.D. Cal. 2004) ("because this savings clause also makes particular reference to notification and recall provisions as non-exclusive remedies," automaker's field and conflict preemption claims run "contrary to the plain language of the statute"). CL ¶¶ 70-71.

C. The 2020 Right to Repair Law Does Not Conflict with the CAA.

The Alliance's implied preemption claim under the CAA fares no better. First, the statute and its regulations make clear that it is the purpose of Congress to *require* open access to emissions-control data—not, as the Alliance contends, to prohibit such access because it might facilitate tampering.[1] The fact that the CAA requires the facilitation of access to vehicle data for

[1] *See* 42 U.S.C. § 7521(m)(5) (directing EPA to require OEMs to provide to "any person engaged in the repairing or servicing of motor vehicles or motor vehicle engines . . . any and all information needed to make use of the [vehicle's] emission control diagnostic system . . . and such other information including instructions for making emission-related diagnoses and

diagnostic and repair purposes refutes the Alliance's argument that it was "the clear and manifest purpose" of Congress to preempt state laws that do the same thing. *Arizona*, 567 U.S. at 400. CL ¶ 99.

There is no other provision in the CAA or its regulations that regulates vehicle cybersecurity or data access controls. Indeed, FCA's Global Head of Technical Compliance acknowledges that there are no EPA regulations that relate to cybersecurity. FF ¶ 171. To the contrary, the CAA's savings clause expressly preserves the right of states "to control, regulate, or restrict the use, operation, or movement of registered or licensed motor vehicles." 42 U.S.C. § 7543(d). By seeking to standardize access to vehicles' on-board diagnostic systems, the 2020 Right to Repair Law falls well within the saving clause's preservation of state authority to regulate anything that "affects the vehicle's 'quality' and 'method' of functioning (*i.e.*, operation)." *In re Volkswagen "Clean Diesel" Mktg., Sales Practices, & Prods. Liab. Litig.*, 959 F.3d 1201, 1216 (9th Cir. 2020) (citation omitted). CL ¶ 57.

Nor does the 2020 Right to Repair Law conflict with the CAA's anti-tampering prohibition. That provision, which makes it unlawful for "any person to remove or render inoperative any device or element of design installed on or in a motor vehicle or motor vehicle engine in compliance with regulations under this subchapter," prohibits only the disabling of devices or elements required by the Act's emissions standards—not state laws impacting data-

---

repairs"); 40 C.F.R. § 86.1808-01(f)(2)(i) (maintenance instructions requiring that repair shops receive access to "any and all information needed to make use of the on-board diagnostic system and such other information, including instructions for making emission-related diagnoses and repairs," and providing that "[n]o information may be withheld . . . if that information is provided (directly or indirectly) by the manufacturer to franchised dealers or other persons engaged in the repair, diagnosing, or servicing of motor vehicles or motor vehicle engines"); 40 C.F.R. § 86.010-38(j)(3)(i) (same).

access controls that GM or FCA may have superimposed on those federally required devices or elements. *See* 42 U.S.C. § 7522(a)(3)(A). Because no federal standards or regulations require that data-access controls be installed in connection with emission-control devices, the term "any device or element of design" in § 7522(a)(3)(A) cannot be interpreted as referring to such extraneous controls. To the contrary, the anti-tampering prohibition must be read to harmonize with (i) § 7521(m)(5), which, as discussed, mandates that "any and all" information needed to use an emission-control diagnostic system be made available to "any person engaged in the repairing or servicing of motor vehicles or motor vehicle engines"; (ii) the CAA's broad saving clause; and (iii) the presumption "that 'the historic police powers of the States' are not superseded 'unless that was the clear and manifest purpose of Congress.'" *In re Volkswagen*, 959 F.3d at 1219 (quoting *Arizona*, 567 U.S. at 400). CL ¶¶ 97-104.

IV. AS A MATTER OF FACT, GM AND FCA CAN IMPLEMENT THE 2020 RIGHT TO REPAIR LAW WITHOUT VIOLATING THE MVSA OR CAA.

Judgment should also enter in defendant's favor because the evidence at trial will show that there is no irreconcilable conflict between compliance with the 2020 Right to Repair Law and compliance with the MVSA and the CAA. To the contrary, GM or FCA can implement the Massachusetts law in a variety of ways, using established technologies that they already incorporate into their vehicles, without creating security risks. As such, the fundamental factual premise of the Alliance's claims is incorrect.

A. The Evidence Will Show that GM and FCA Are Highly Capable Parties With Strong Preexisting Cybersecurity Capabilities.

The trial evidence will show that the two designated OEMs in this case, GM and FCA, have extensive expertise and knowledge in cybersecurity issues that will allow them to implement the 2020 Right to Repair Law while protecting vehicle safety. GM employs a large

product cybersecurity team consisting of approximately 55 employees. That team ensures that GM's "foundational" cybersecurity suite applies to all complex, sensitive, or safety-critical ECUs in any GM vehicle. FF ¶¶ 118-30. FCA similarly uses a variety of tools and strategies to protect the cybersecurity of its vehicles. *See* FF ¶¶ 162-68.

B. The Evidence Will Show that, in View of Their Strong Preexisting Capabilities, GM and FCA Have Multiple Potential Methods to Comply with the Massachusetts Law.

1. GM and FCA have multiple potential methods to comply with Section 2.

Section 2 of the 2020 Right to Repair Law amends Mass. Gen. Laws ch. 93K, § 2, which currently requires OEMs to provide access to vehicle on-board diagnostic systems. The new law adds a paragraph requiring that "motor vehicle owners' and independent repair facilities' access to vehicle on-board diagnostic systems" be "standardized and not require any authorization by the manufacturer, directly or indirectly," unless that authorization system "is standardized across all makes and models sold in the Commonwealth and is administered by an entity unaffiliated with a manufacturer." CL ¶ 40.

The term "authorization," as it appears in Section 2, is a technical term of art, the meaning of which the Attorney General has supported with evidence in the form of expert opinion. Specifically, "authorization" refers to an actor's role or what an actor is and is not permitted to do on a system. Authorization is distinct from authentication, which refers to the confirmation of the identity of an individual, user, or other actor. FF ¶¶ 54-55; CL ¶¶ 40-42. Where a statute uses a technical "term of art" with an established meaning in an industry, courts "assume" that the Legislature or, in the case of a ballot initiative, the voters, "intended it to have its established [technical] meaning," absent any contrary indication. *McDermott Int'l, Inc. v. Wilander*, 498 U.S. 337, 342 (1991). Furthermore, because she has authority to enforce the 2020

Right to Repair Law, the Attorney General's interpretation of the law's terms is entitled to "great weight." *McGuire v. Reilly*, 386 F.3d 45, 55, 64 (1st Cir. 2004). CL ¶¶ 31-33.

Because Section 2 only requires that authorization to a vehicle's on-board diagnostic system be administered by an unaffiliated entity, it does not limit the ability of an OEM to require authentication. Any access control or other safety technique that does not require authorization by the OEM can continue to be implemented in vehicles. CL ¶¶ 43-44. For example, a common technique that does not require OEM authorization are vehicle condition checks, or "rationality" checks. *See* FF ¶¶ 109-11. As expert Brian Romansky will explain, these checks are performed within existing vehicle ECUs to confirm that certain conditions are met before a particular diagnostic or repair procedure is allowed. An anti-lock brake system may enable a diagnostic procedure only when the vehicle is parked and stationary, which would prevent a malicious actor from manipulating the brakes while the car is in motion. This type of vehicle condition check does not require authorization because the OEM is not involved in individual instances of deciding whether access to perform a certain action is allowed.

The trial evidence will show that an OEM such as GM or FCA can comply with Section 2 without violating federal law. Some OEMs already provide standardized access to their on-board diagnostic systems and do not require either direct or indirect manufacturer authorization. Standardized access to their on-board diagnostic systems is provided by the J-1962 connector. Those OEMs will not have to make any changes to comply with this provision, and that fact alone shows that compliance with Section 2 and federal law is not impossible. FF ¶¶ 7-8, 175; CL ¶¶ 79, 90-91.

The subset of OEMs that wish to continue to require authorization to access vehicle on-board diagnostic systems will need to establish an authorization system that is "administered by

an entity unaffiliated with a manufacturer." The Attorney General interprets the phrase "an entity unaffiliated with a manufacturer" to exclude entities that have a formal corporate affiliation with the manufacturer or are subject to direct or indirect control by a manufacturer. FF ¶ 56; CL ¶ 45. Expert Brian Romansky will detail methods by which such an authorization system can be developed using public key infrastructure (PKI) technology and authentication techniques. These methods do not compromise the security or integrity of vehicle networks and do not require removal of access controls. Rather, they require replacing one access control—manufacturer authorization to access the on-board diagnostic system—with an authorization system that is secure but administered by an entity unaffiliated with the OEM. Administration of PKI systems by an unaffiliated entity is common and well-established in other industries, such as internet web browsers. FF ¶¶ 18-27, 176-88; CL ¶¶ 92. Expert Craig Smith will describe how a standardized third-party method can authorize the requisite level of access necessary for repair shops to diagnose and make all necessary repairs, potentially by managing the certificate approvals for tool manufacturers.

The Right to Repair law leaves the decision of how to set up the authorization system administered by an unaffiliated entity up to the OEMs, so they are free to work with any unaffiliated entity they choose. Myriad unaffiliated entities could provide this function. For example, the Equipment and Tool Institute (ETI) currently acts as a third-party entity that administers authorization/vetting for third-party diagnostic scan tool companies. ETI and vehicle manufactures have an existing relationship, and ETI is one unaffiliated entity that could provide standardized authorization of repair tools. Another viable unaffiliated entity is the National Automotive Service Task Force (NASTF), an independent organization that facilitates cooperation between OEMs and the aftermarket, and handles things such as authorizing

replacement keys for locksmiths. NASTF's existing Secure Data Release Model (SDRM) program verifies the business, checks insurance, and performs background checks to validate the vehicle owner or business, and could be expanded to issue encryption keys on behalf of OEMs after validating a vehicle owner or tool manufacturer. FF ¶¶ 189-95; CL ¶¶ 79-80, 92.

2. GM and FCA have multiple potential methods to comply with Section 3.

Section 3 of the 2020 Right To Repair Law further amends Mass. Gen. Laws ch. 93K, § 2, by replacing subparagraph (f), which exempted certain telematics systems data, with a new subparagraph (f), which provides for owner and independent-repair-facility access to mechanical data in cars with telematics systems.[2] For vehicles that have a telematics system and are sold in Massachusetts, Section 3 requires OEMs to equip the vehicles—starting with model year 2022—with an "inter-operable, standardized and open access platform," which "shall be capable of securely communicating" mechanical data from the vehicle "via direct data connection to the platform." Vehicle owners will have access to this platform through a mobile-based application. Independent repair facilities and new car dealerships will have access to the vehicle's mechanical data to perform maintenance and repairs, with the owner's authorization, limited to the time needed to complete the repair or another period of time agreed to by the owner for the purposes of maintaining, diagnosing and repairing the motor vehicle. During this period, independent

[2] Pursuant to Section 1 of the 2020 Right to Repair Law, "mechanical data" encompasses "any vehicle-specific data, including telematics system data, generated, stored in or transmitted by a motor vehicle used for or otherwise related to the diagnosis, repair or maintenance of the vehicle." Also pursuant to Section 1, "telematics system" in this definition means "any system in a motor vehicle that collects information generated by the operation of the vehicle and transmits such information, in this chapter referred to as 'telematics system data,' utilizing wireless communications to a remote receiving point where it is stored." Mechanical data thus includes the vehicle's pre-defined diagnostic functions and any data generated, stored, or transmitted by the vehicle and used for vehicle diagnostics, maintenance, or repair. FF ¶¶ 50-52; CL ¶¶ 35-38.

repair facilities and new car dealerships will also be able to send commands to the vehicle if needed for the purposes of maintenance, diagnostics, and repair. FF ¶¶ 57-58; CL ¶ 46.[3]

The trial evidence will show that an OEM such as GM or FCA has several potential ways to comply with Section 3 without violating federal law. First, Section 3 requires vehicles to be equipped with an inter-operable, standardized, and open access platform only if the vehicle "utilizes a telematics system." If a vehicle is not equipped with a telematics system, or if the OEM disables a vehicle's telematics system, Section 3 does not require that it be equipped with an inter-operable, standardized, and open access platform. Some vehicles are not equipped with a telematics system, and those vehicles will not require any changes. For vehicles that are equipped with telematics systems, as expert Craig Smith will testify, there are at least three ways OEMs can disable those systems: (1) by modifying the configuration, (2) by disabling the "dialing services" that control external communication, or (3) by disabling the cellular access via the telematics provider. None of these methods would adversely impact vehicle security. To the contrary, because a telematics system provides an additional "attack surface," disabling that system would actually increase the vehicle's security. FF ¶¶ 196-205; CL ¶¶ 81, 93-94.

Alternatively, an OEM can either design and equip its telematics-enabled vehicles with

[3] Several terms that appear in Section 3 are technical terms of art, the meaning of which the Attorney General has supported with evidence in the form of expert opinion. "Platform" refers to the vehicle architecture and associated software/features. To be "interoperable" means a standard way to connect and communicate with the vehicle. An interoperable device is one that can be used regardless of the manufacturer. To be "standardized" means to follow a common and well documented method to perform the necessary actions such that there is a common, agreed upon way of communicating. To be "open access" means to have a non-gated way to gain access to the data and capabilities. Open access requires the platform and the mechanical data it communicates with to be freely accessible to the owner, without the OEM acting as a gatekeeper. To be "directly accessible" means that the consumer will not need to go through the OEM to perform diagnosis, maintenance, and repairs. FF ¶¶ 59-65; CL ¶¶ 47-51.

an inter-operable, standardized, and open access platform, or modify its existing systems to create such a platform. While the information necessary to design the platform, or modify a vehicle's existing systems to create such a platform, is exclusively within each OEM's possession, custody, and control, the Attorney General's experts will discuss feasible possibilities for designing such a platform. FF ¶¶ 206; CL ¶¶ 95.

One possible platform is the SAE J-1962 connector with the addition of an OBD-connected telematic "dongle." The J-1962 connector is a known and equally-accessible way to gain access to a vehicle's diagnostic functionality. Existing passenger vehicle dongles can currently send and receive information through the J-1962 connectors. For vehicles that include incorporate a gateway module, the dongles could be provided with the appropriate access level requirements to send and receive commands. In the case of a role-based key or certificate form of security, a dongle could be issued a key to match the dongle's intended capabilities for diagnosis, maintenance, and repair. Regardless of whether a vehicle has a gateway module, other security measures in use by OEMs, such as ECU authentication and message authentication, can stay in place under this compliance option, provided that the authorization aspects of those security measures are administered by an entity unaffiliated with an OEM as required by Section 2. FF ¶¶ 207-19; CL ¶¶ 82, 95.

Another compliance option is for OEMs to develop, in the coming years, a fully telematic platform to support remote diagnostics. Because a telematic platform has an increased attack surface due to its wireless nature, such a telematic platform would need to employ additional security. Core controls would likely involve segmentation / isolation, authentication, authorization, and encryption. For vehicles that already have gateways and telematics systems segmented into their network, OEMs would need to develop, test, and deploy a new version of

firmware (embedded software) to upgrade the existing telematics systems. For other OEMs and vehicles that do not already have segmented vehicle architectures, gateways, encryption capabilities, or other features required for a secure telematic platform, compliance under this option would require more time to design, test, and validate the necessary architectural changes. FF ¶¶ 220-28; CL ¶¶ 83, 95.

None of these compliance options would create security risks to the vehicles, much less require OEMs to violate the MVSA or the CAA. CL ¶¶ 83, 95-96. Each approach would allow independent repair facilities and vehicle owners to access a vehicle's mechanical data, including "the ability to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics, and repair" as Section 3 requires.[4] This ability can be given in a way that preserves security and enables repair shops and vehicle owners to make necessary repairs. Each compliance option would also allow mechanical data to be "securely communicated," as required by Section 3.[5] One standardized method for securely communicating mechanical data is the Secure Vehicle Interface or "SVI," a technical design pattern developed to support an interoperable interface for diagnostic and repair data. The SVI design is documented in three technical standards published jointly by the European Committee for Standardization and the

[4] The Attorney General interprets the phrase "ability to send commands to in-vehicle components if needed for purposes of maintenance, diagnostics and repair" in Section 3 to mean the ability to write diagnostic data to electronic control units in a vehicle, and transmit packets to the electronic control unit, if necessary for the maintenance, diagnosis, or repair of a vehicle. FF ¶ 67; CL ¶ 52.

[5] The Attorney General interprets the term "securely communicated" in Section 3 to mean communication in a way that authenticates the identities of the recipient and the sender, where the communication is not made known to parties other than the recipient and the sender and the integrity of the communication is not compromised. FF ¶ 68; CL ¶ 53.

International Organization for Standardization. FF ¶¶ 229-35.[6]

C. The Evidence Will Show that Both GM and FCA Have Ulterior Motives for Resisting the 2020 Right to Repair Law, that GM Has Made No Meaningful Attempt to Find a Feasible Way to Comply with the Law, and that FCA Believes It Can Comply with the Law.

Finally, it is significant that the Alliance's members such as GM and FCA have had ample notice of the 2020 Right to Repair Law's requirements, but have not taken reasonable steps to prepare to comply with the law. As early as 2015, aftermarket associations began discussions with the Alliance's predecessor organizations about providing independent repair facilities with secure access to telematics system data. In 2016, the leading aftermarket trade association, the Auto Care Association, began delivering technical presentations to the Alliance's predecessor organizations, as well as to individual OEMs, including GM, about SVI. From 2015 to the present, the OEMs have refused to work with the Auto Care Association to implement SVI. They have also refused to develop their own methods of providing secure access to telematics system data to independent repair facilities. FF ¶¶ 42-45.

By September 2019, when the Attorney General certified that the ballot question complied with state constitutional requirements, GM and FCA knew the precise language that would appear on the ballot. FF ¶¶ 46-47. Even then, they did not take reasonable steps to prepare to comply with the ballot question if it passed, even though the previous right to repair

[6] The ISO 21177 standard defines a method of adapting the widely used Transport Layer Security (TLS) mechanism to utilize the IEEE 1609.2 certificate architecture. The ISO 21184 standard defines a data dictionary, or a way to translate between proprietary, vehicle-specific messages and protocols and a standard, published set of external message types. The ISO 21185 standard defines a standard set of communication profiles that can be enabled using conventional wireless technologies including WiFi, 4G and 5G cellular, and other common wireless connection methods. Together, ISO 21184 and ISO 21185 provide an interface to translate a vehicle's existing, proprietary internal messages into a common external interface that can be easily shared with tool vendors. FF ¶¶ 236-42.

ballot question passed overwhelmingly, with 86% of voters in favor. FF ¶¶ 35-36. Instead, after the 2013 Right to Repair Law was enacted, more OEMs equipped their vehicles with telematics systems, which gave OEMs new ways to control the mechanical data of their customers' cars after selling the cars. FF ¶¶ 40-41.

GM and FCA have had years of lead time to design, test, and implement, any design changes necessary to comply with the 2020 Right to Repair Law. Their refusal to use this time is not grounds for impossibility preemption. To the contrary, the evidence will show that in November 2020, soon after the voters approved the 2020 Right to Repair Law, [redacted]. *See* FF ¶¶ 135-52. (The details of these discussions are shielded by GM's confidentiality designations.) As for FCA, its Global Head of Technical Compliance, drawing on his "vast experience," believes that FCA could design a platform of the type contemplated by the 2020 Right to Repair Law, and could probably do so within a two-year window. FF ¶ 172.

CONCLUSION

The preemption claims of the plaintiff Alliance for Automotive Innovation fail as a matter of law, and the evidence at trial will further establish that OEMs can comply with the 2020 Right to Repair Law without violating the MVSA or the CAA. Accordingly, the Alliance's request for injunctive and declaratory relief should be denied, and judgment should enter in favor of the Attorney General.

Respectfully submitted,

MAURA HEALEY
ATTORNEY GENERAL,

/s/ Robert E. Toone
Robert E. Toone, BBO No. 663249
Eric A. Haskell, BBO No. 665533
Phoebe Fischer-Groban, BBO No. 687068
Julia Kobick, BBO No. 680194
Assistant Attorneys General
Christine Fimognari, BBO No. 703410
Special Assistant Attorney General
One Ashburton Place
Boston, Massachusetts 02108
(617) 963-2178
Robert.Toone@mass.gov

Dated: June 4, 2021

CERTIFICATE OF SERVICE

I hereby certify that this document, filed through the ECF system, will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and that paper copies will be sent to those indicated as non-registered participants on June 4, 2021.

/s/ Robert E. Toone